IoT機器を狙ったサイバー攻撃の現状とNICTの取り組み

井上 大介
国立研究開発法人 情報通信研究機構
サイバーセキュリティ研究所
サイバーセキュリティ研究室

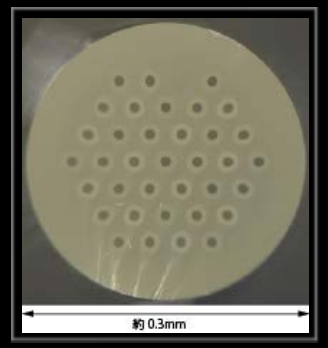
NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

国立研究開発法人 情報通信研究機構とは？

● 情報通信分野を専門とする日本で唯一の公的研究機関

日本標準時の生成・配信
（うるう秒挿入）

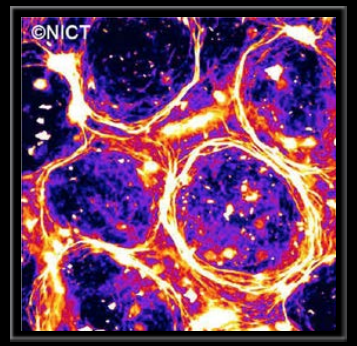


光通信システム
（ペタbps級 マルチコアファイバ）

宇宙通信システム
（超高速インターネット衛星きずな）

サイエンスクラウド
（ひまわり8号リアルタイムWeb）

電磁波センシング
（Pi-SAR2による3.11直後の仙台空港）



バイオ・ナノICT
（生体分子の自己組織化）

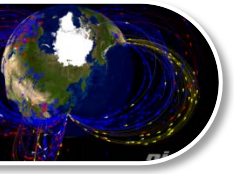
脳情報通信融合
（ブレイン・マシーン・インターフェイス）

多言語音声翻訳
（多言語音声翻訳アプリVoiceTra）

超臨場感コミュニケーション
（初音ミクさんの電子ホログラフィ）

サイバーセキュリティ
（対サイバー攻撃アラートシステムDAEDALUS）

サイバーセキュリティ研究室 研究マップ



インシデント分析センタ（ニクター）

NICTER

対サイバー攻撃アラートシステム（ダイダロス）

DAEDALUS

受 Passive

サイバー攻撃統合分析プラットフォーム（ニルヴァーナ・カイ）

NIRVANA改

脆弱性管理プラットフォーム（ニルヴァーナ・カイ・ニ）

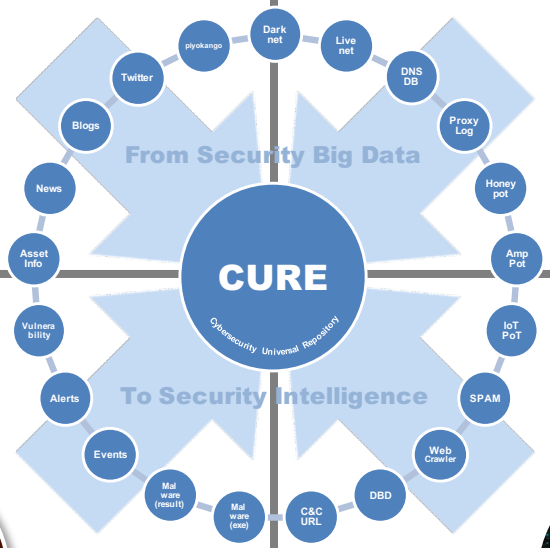
NIRVANA改弐

Global (無差別型攻撃対策)

(標的型攻撃対策) Local

全

局



サイバーセキュリティ
ユニバーサル・リポジトリ
CURE

能

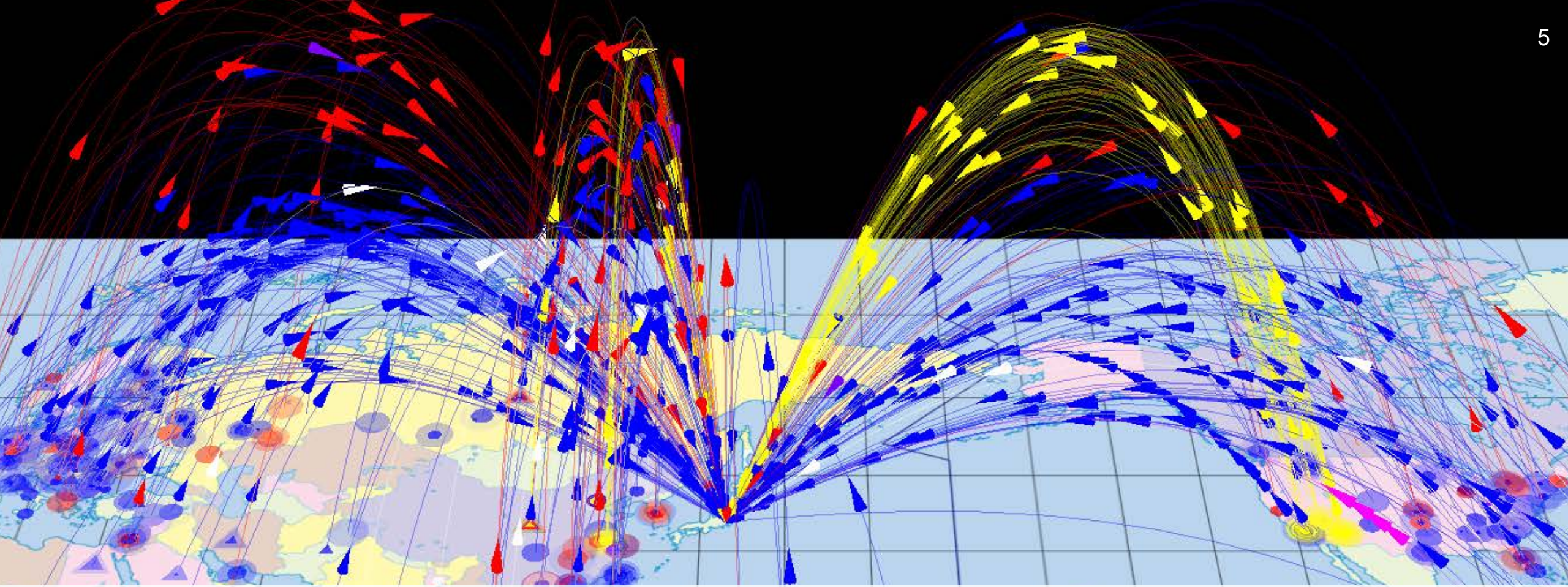
Active

NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

インシデント分析センター

Network **I**ncident analysis **C**enter for **T**actical **E**mergency **R**esponse

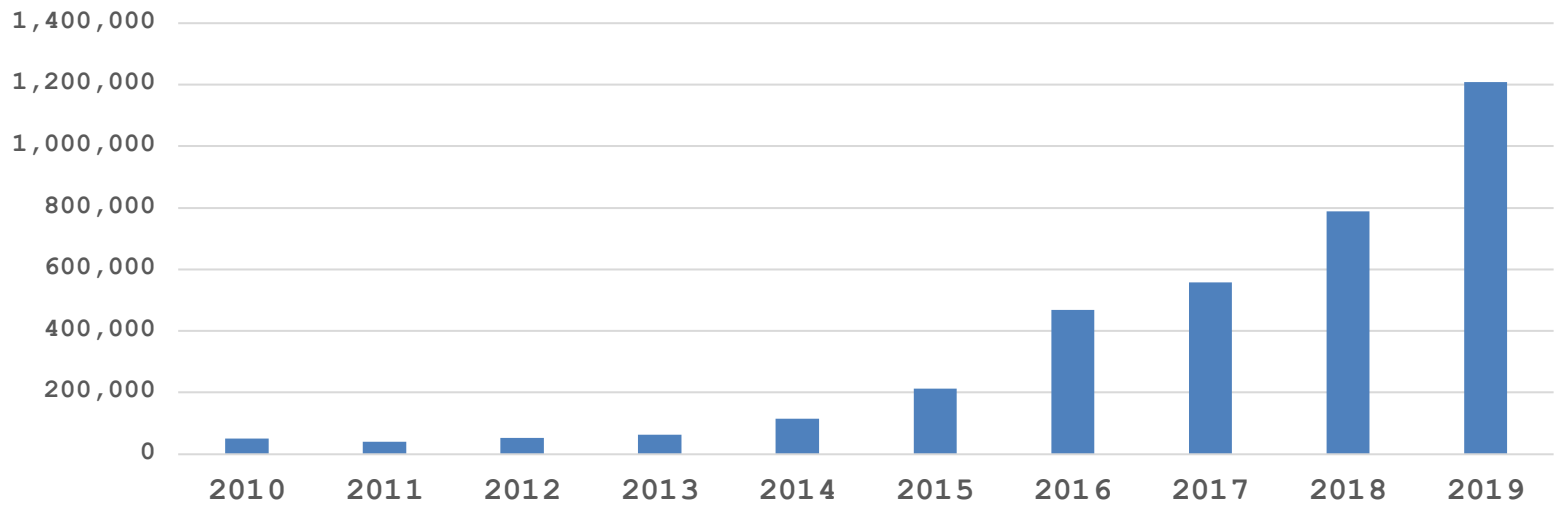


NICTER

- サイバー攻撃リアルタイム大規模観測・分析システム
- 国内外で30万の未使用IPアドレス“**ダークネット**”を観測
- 無差別型サイバー攻撃の大局的な傾向把握に有効

NICTERダークネット観測統計（過去10年）

年	年間総観測パケット数	ダークネットIPアドレス数	1 IPアドレス当たりの年間総観測パケット数
2010	約56.5億	約12万	50,128
2011	約45.4億	約12万	40,654
2012	約77.8億	約19万	53,085
2013	約128.8億	約21万	63,655
2014	約256.6億	約24万	115,323
2015	約545.1億	約28万	213,523
2016	約1,281億	約30万	469,104
2017	約1,504億	約30万	559,125
2018	約2,121億	約30万	789,876
2019	**約3,279億**	**約30万**	**1,209,112**



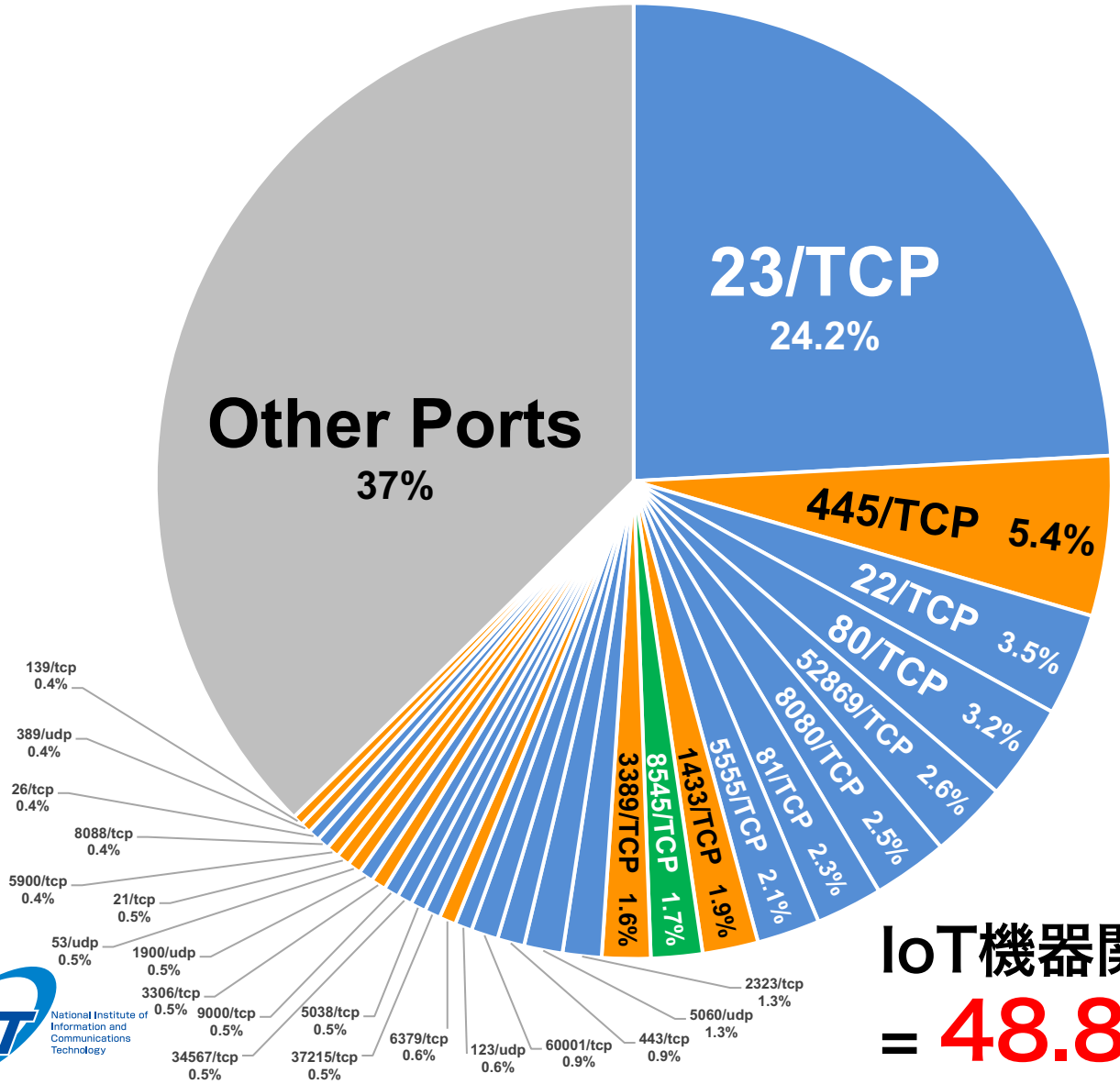
National Institute of Information and Communications Technology

Network Incident analysis Center for Tactical Emergency Response


IoT
Internet of Things
横浜国立大学
吉岡研究室による調査
7
YNU
HG8245
嵌入式電話錄音主機WEB管理系統
V1.0
Java Application
Web Application
pandora
Login
Username:
Password:
RouterOS v5.22
MikroTik
BISBOX
DiskStationPlay
Aanmelden
11n 150Mbps WLAN ADSL2+ Modem Router
Status
Network
Wireless
DrayTek
ZTE中兴
F460
Welcome To Streamyx Connection Setup
Network video client
LOGIN

感染機器の分布（2019年）

- NICTER 観測レポート 2019：宛先ポート番号別パケット数分布 -



Top10ポート	攻撃対象
23/TCP	IoT機器 （Webカメラ等）
445/TCP	Windows（サーバサービス）
22/TCP	IoT機器（ルータ等） 認証サーバ（SSH）
80/TCP	Webサーバ（HTTP） IoT機器（Web管理画面）
52869/TCP	IoT機器（ホームルータ等）
8080/TCP	IoT機器（Webカメラ等）
81/TCP	IoT機器（ホームルータ等）
5555/TCP	Android 機器 （セットトップボックス等）
1433/TCP	Windows（MS-SQL）
8545/TCP	イーサリアム（仮想通貨）

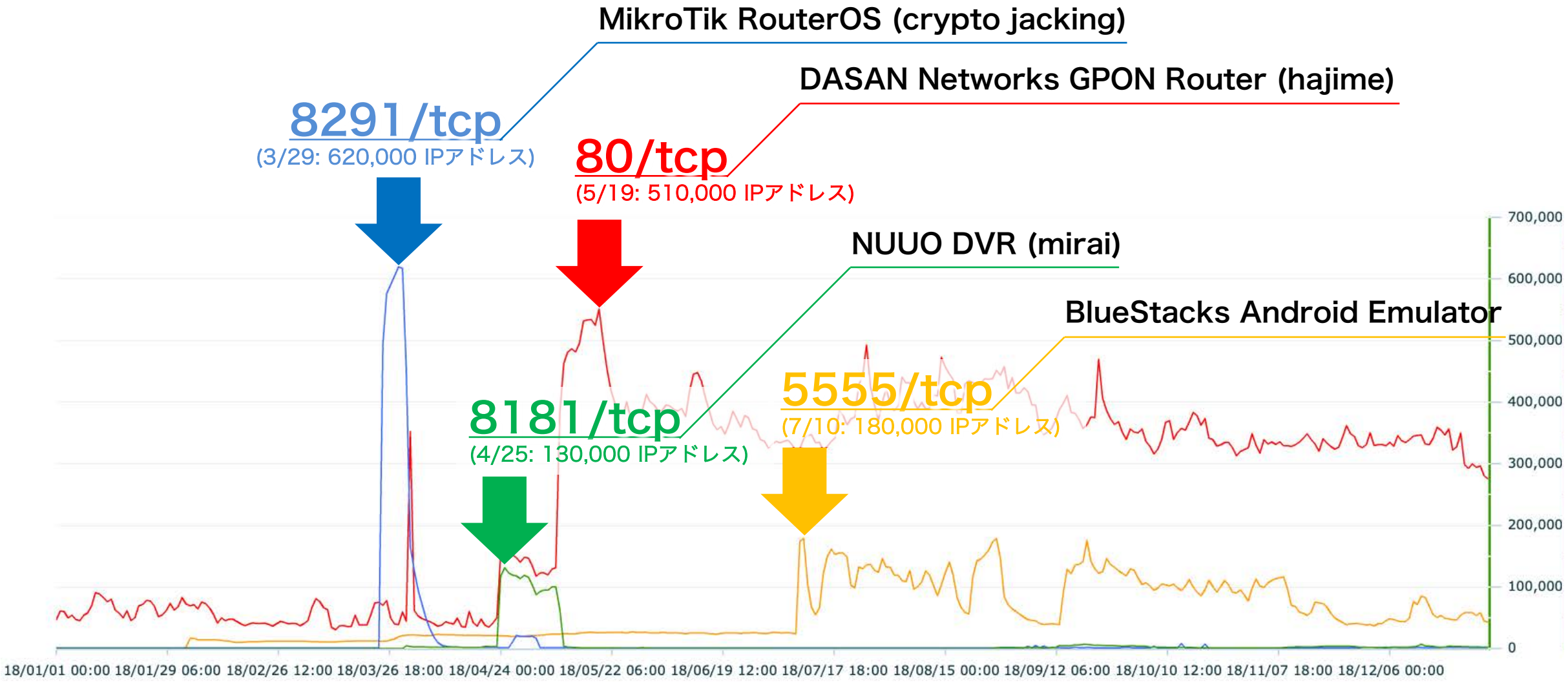
IoT機器関連ポート

= 48.8%（上位30ポート中）

NICT National Institute of Information and Communications Technology

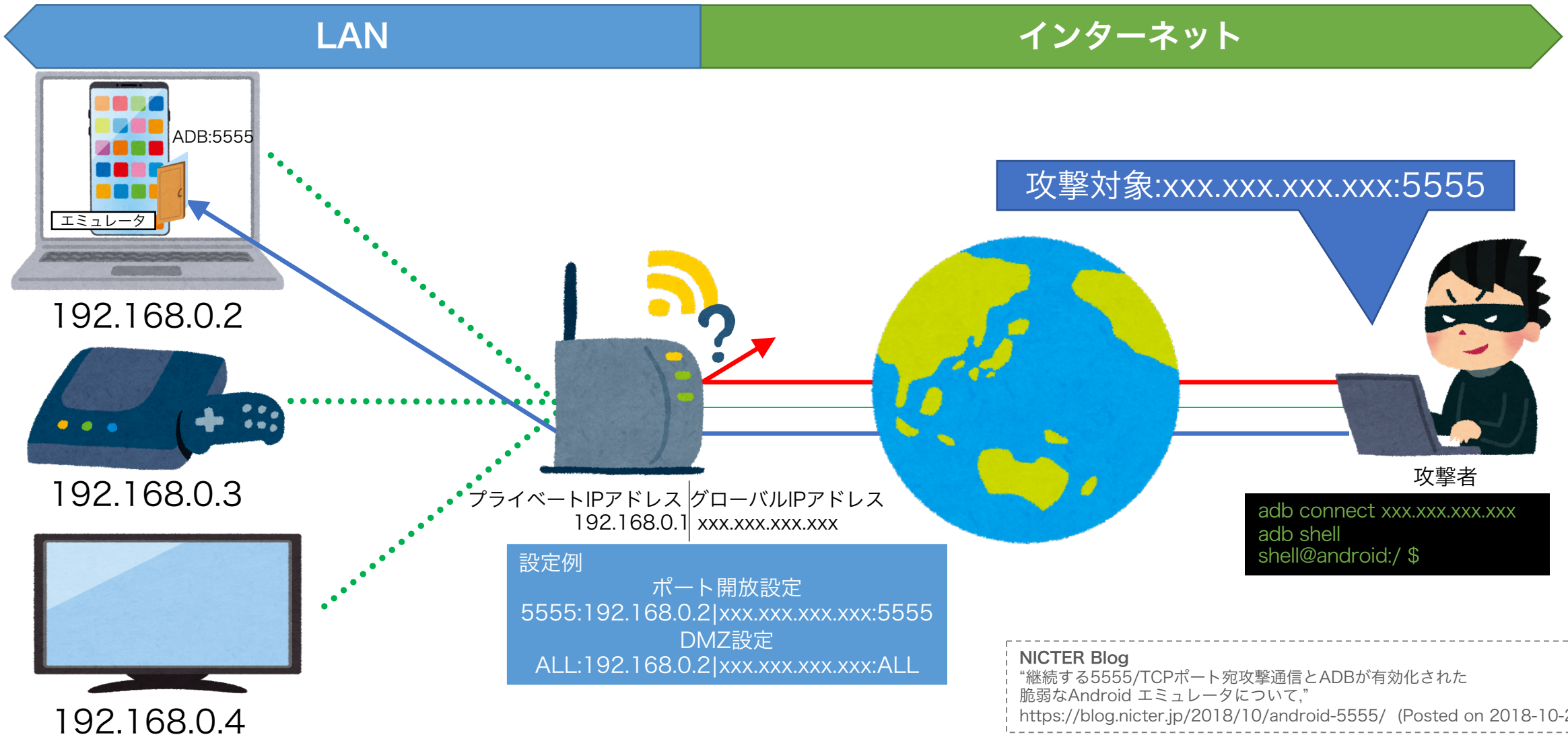
NICTER Network Incident analysis Center for Tactical Emergency Response

2018年の主な大規模感染事例



ユニークホスト数/日（2018年1月～12月）

脆弱なAndroidエミュレータを狙った攻撃（5555/TCP）

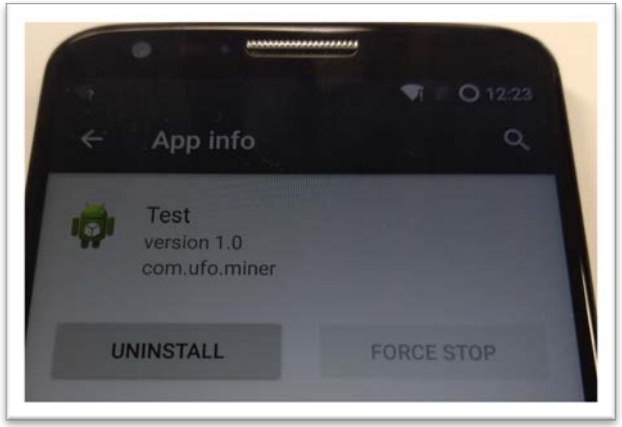


NICTER Blog
“継続する5555/TCPポート宛攻撃通信とADBが有効化された脆弱なAndroid エミュレータについて,”
https://blog.nicter.jp/2018/10/android-5555/ (Posted on 2018-10-22)

ポート開放等の設定をしていない場合（赤色）：攻撃者からのグローバルIPアドレスへの通信は、プライベートIPアドレスへ変換できないため通信できない。
ポート開放 をしている場合（青色）：攻撃者からのグローバルIPアドレスへの通信をプライベートIPアドレスへ変換するため、エミュレータへ転送してしまう。

5555/TCP経由で感染するマルウェア

- **仮想通貨採掘 Android アプリ（apkファイル）**
  - ✓ 感染端末上で仮想通貨の採掘を行うマルウェア
  - ✓ 同一アプリ（com.ufo.miner）を1年以上継続的に観測



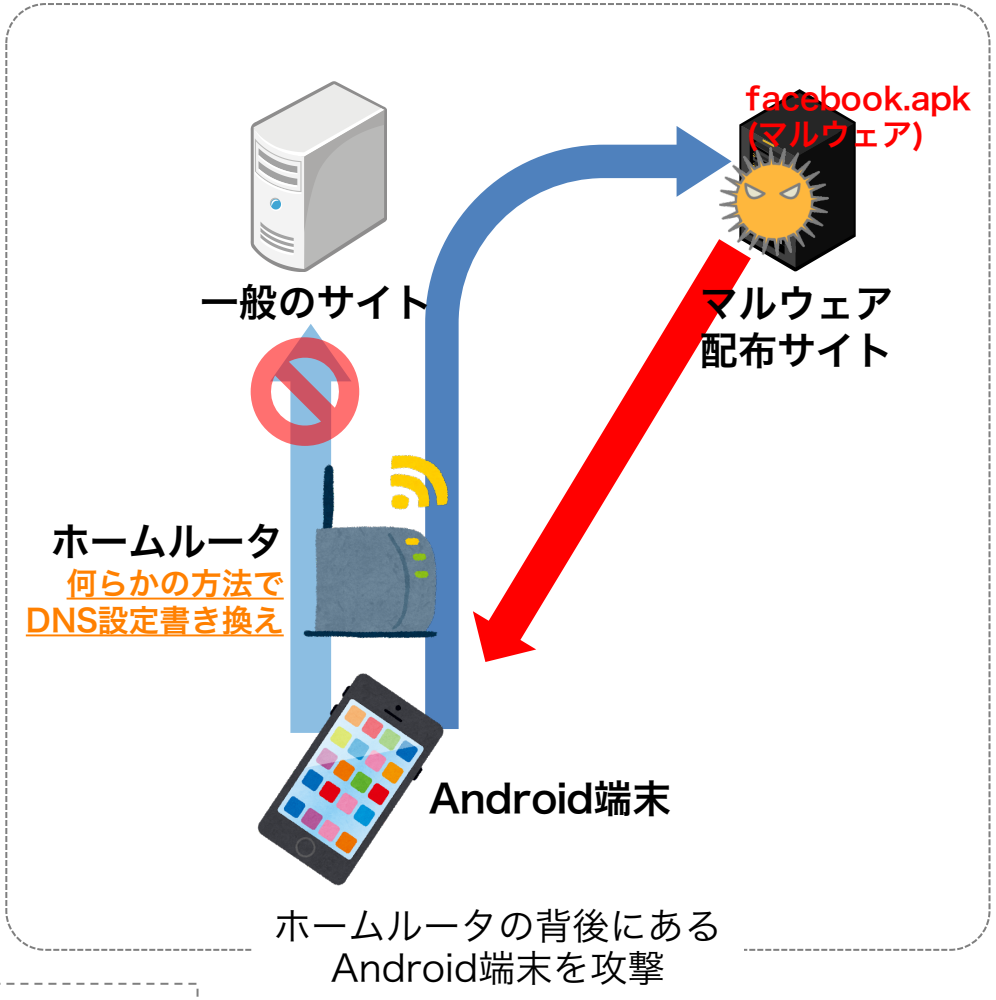
- **DDoS攻撃を行うマルウェア**
  - ✓ Android端末から1日26GBの大量通信が発生するケースも
  - ✓ 攻撃命令を出すC&Cサーバは１か月以上稼働

- **ADBポート等のパケットフィルタリングを行うマルウェア**
  - ✓ 他のマルウェアによる感染を防止し感染を永続化

```
[dhcp161:Downloads yoshiki$ strings initdz | grep DROP
 iptables -A OUTPUT -p tcp --dport 3333 -j DROP
 iptables -A OUTPUT -p tcp --dport 5555 -j DROP
 iptables -A OUTPUT -p tcp --dport 7777 -j DROP
 iptables -A OUTPUT -p tcp --dport 9999 -j DROP
 iptables -A OUTPUT -p tcp --dport 14444 -j DROP
```

高度化するIoT機器への攻撃

- 2016年以前
  - デフォルトID/パスワードでログインし感染
- 2017年
  - デフォルトID/パスワードでログインし感染
  - IoT機器の脆弱性を攻撃して感染
- 2018年
  - デフォルトID/パスワードでログインし感染
  - IoT機器の脆弱性を攻撃して感染
  - IoT機器の背後にある機器を攻撃

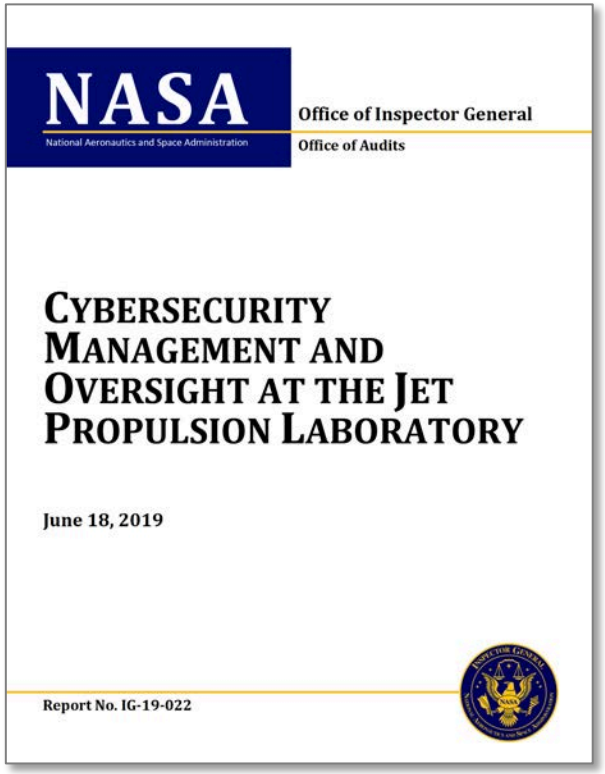


ホームルータの背後にある
Android端末を攻撃

NICTER Blog
"Wi-Fi ルータの DNS 情報の書換え後に発生する事象について,"
https://blog.nicter.jp/2018/03/router-dns-hack/ (Posted on 2018-03-26)

NASAへのサイバー攻撃（2019）

- NASAのジェット推進研究所（JPL）から機密データ漏洩
- 無許可接続されたRaspberry Piが原因（野良IoT）


NASA
National Aeronautics and Space Administration
Office of Inspector General
Office of Audits

CYBERSECURITY MANAGEMENT AND OVERSIGHT AT THE JET PROPULSION LABORATORY

June 18, 2019

Report No. IG-19-022


itmedia.co.jp

NASA、サイバー攻撃で機密データ流出　侵入口は無許可接続の「Raspberry Pi」 - ITmedia NEWS

ITmedia NEWS > セキュリティ > NASA、サイバー攻撃で機密データ流出　侵入口は無許...

NASA、サイバー攻撃で機密データ流出　侵入口は無許可接続の「Raspberry Pi」

2019年06月23日 07時45分 公開　[ITmedia]

印刷　1905　Share　B!　828

米航空宇宙局（NASA）のジェット推進研究所（JPL）の研究データが昨年、サイバー攻撃により盗まれていたことが、米連邦政府の監察総監室（OIG）が6月18日付で公開した報告書（リンク先はPDF）で明らかになった。

2018年4月にJPLのネットワークに侵入した攻撃者が約10カ月の間ネットワーク内の多数の脆弱性を利用して行動範囲を広げ、火星科学研究探査機のデータを含む約500MBの機密データを盗んだ。深宇宙通信情報網DSN（ディープスペースネットワーク）のデータにもアクセスした痕跡があるため、JPLのネットワークからDSNの宇宙飛行関連システムを切断したという。

攻撃者の侵入口はJPLのネットワークに無許可で接続していたRaspberry Pi端末だった。本来ならば最高情報責任者室（OCIO）がネットワークに接続するすべての端末を管理しているはずだが、正常に機能していなかった。管理者の1人はOIGに対し、新たに端末を接続する際はセキュリティデータベースに手動で登録することになっているが、更新機能がうまく動かないことがあり、そのまま登録を忘れることがあると語ったという。

Deep Space Network Dish in Goldstone, California
Source: NASA.
DSNのパラボラアンテナ（画像：NASA）


gigazine.net

NASAの機密データがRaspberry Piを侵入口として盗まれたと判明 - GIGAZINE

GIGAZINE

19万点超 著作権フリー音楽
日本最大級のBGM・効果音販売サービス「オーディオストック」 - Audiostock

2019年06月25日 19時00分　セキュリティ

NASAの機密データがRaspberry Piを侵入口として盗まれたと判明

by Les Pounder

アメリカ航空宇宙局(NASA)は、2018年にジェット推進研究所(JPL)のネットワークがハッキングされたことを確認しました。報告によると、ハッキングをしかけたクラッカーは、JPLのネットワークに無許可で接続されたRaspberry Piを侵入口として、データを盗み出したとのことです。

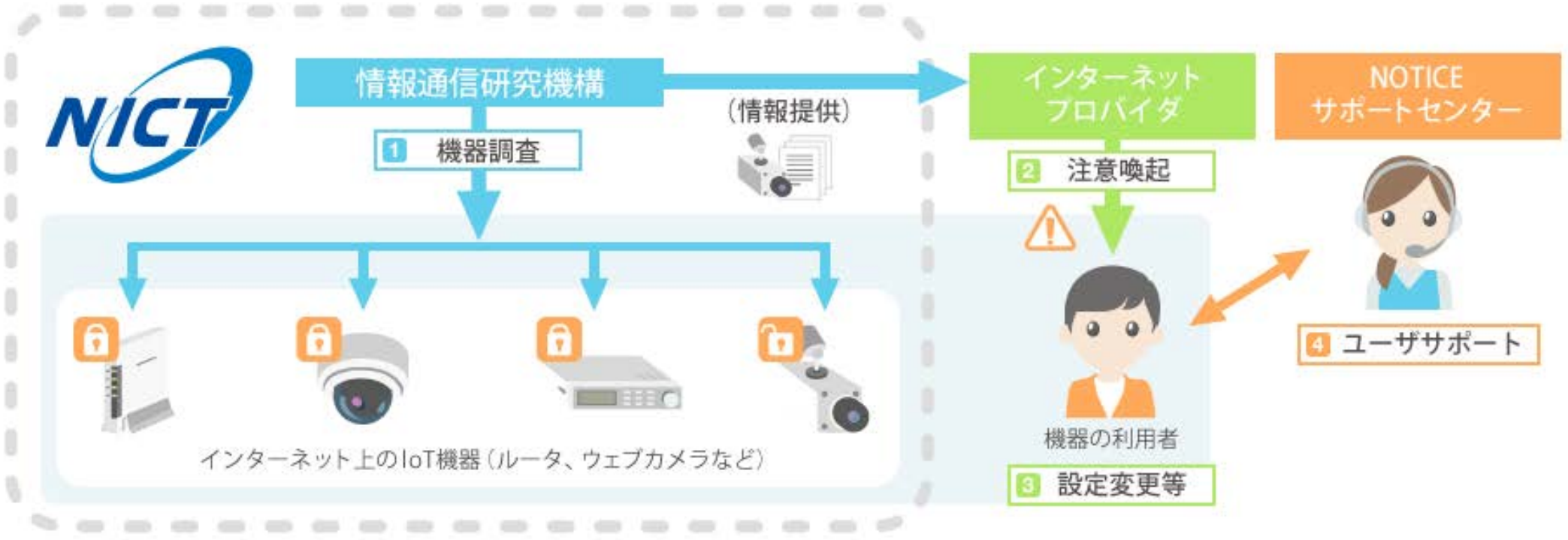
https://oig.nasa.gov/docs/IG-19-022.pdf
https://www.itmedia.co.jp/news/articles/1906/23/news012.html
https://gigazine.net/news/20190625-nasa-hacked-raspberry-pi/

NOTICE

National Operation Towards IoT Clean Environment

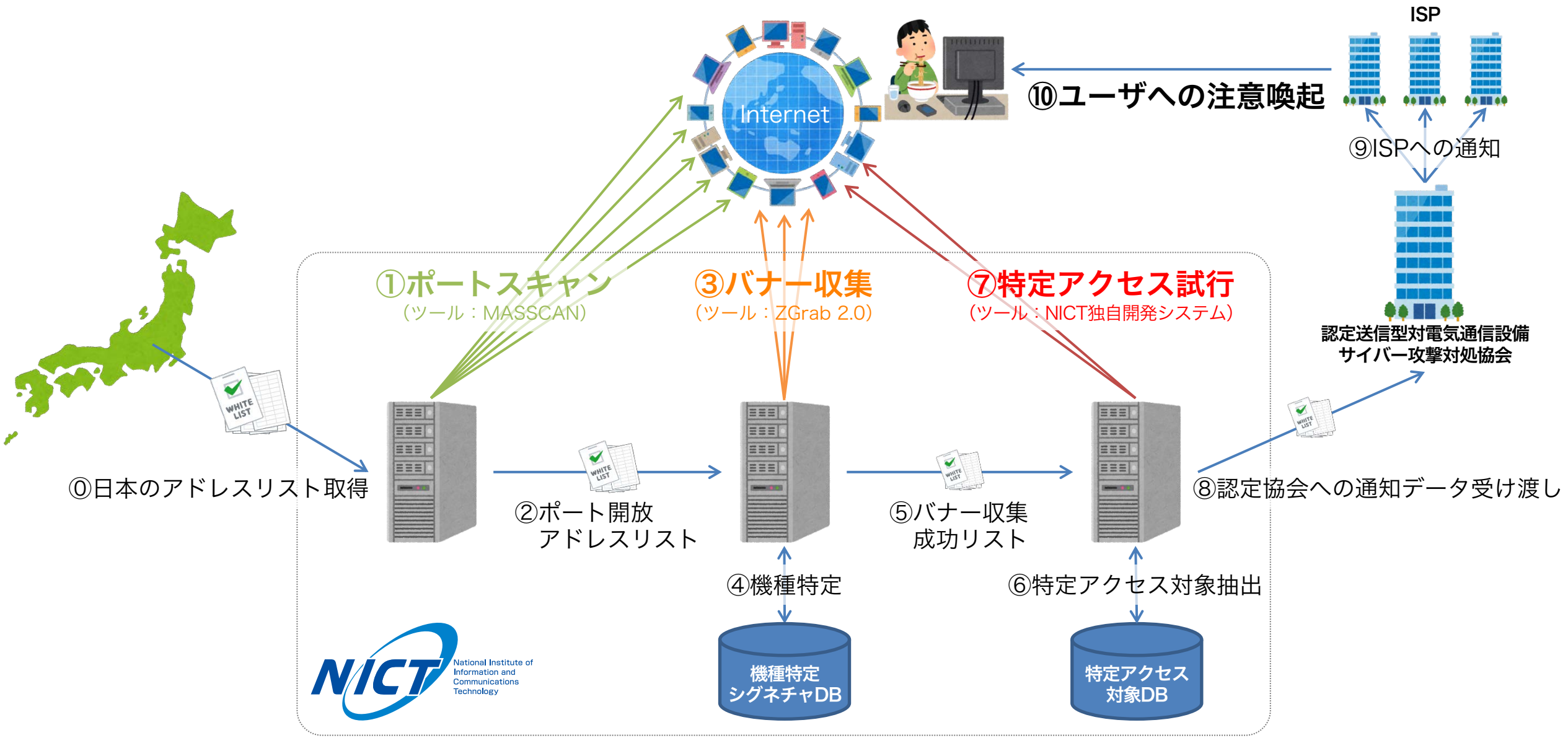
NOTICE

- NOTICE: National Operation Towards IoT Clean Environment
- 総務省、NICT、ISPが連携し、サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起を行う取組



https://notice.go.jp/

NICTによるIoT機器調査の技術詳細



能動的対策と受動的対策

能動的対策

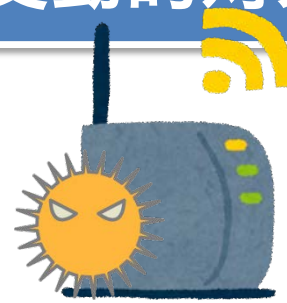
パスワード設定等に
不備があるIoT機器

能動的観測

NOTICE
National Operation Towards IoT Clean Environment

通知

受動的対策

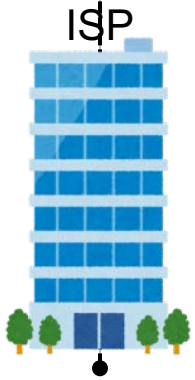


感染IoT機器

受動的観測

NICTER

通知



ISP

IoT機器調査及び利用者への注意喚起の実施状況（2020年７月度）

- 参加手続きが完了している**ISP**（インターネット・サービス・プロバイダ）は**58社**。
  当該ISPの**約1.1億IPアドレス**に対して調査を実施。
- **NOTICE**による注意喚起は、**３３８件**の**対象を検知**しISPへ通知。
- **NICTER**による注意喚起は、１日平均**２０９件**の**対象を検知**しISPへ通知。

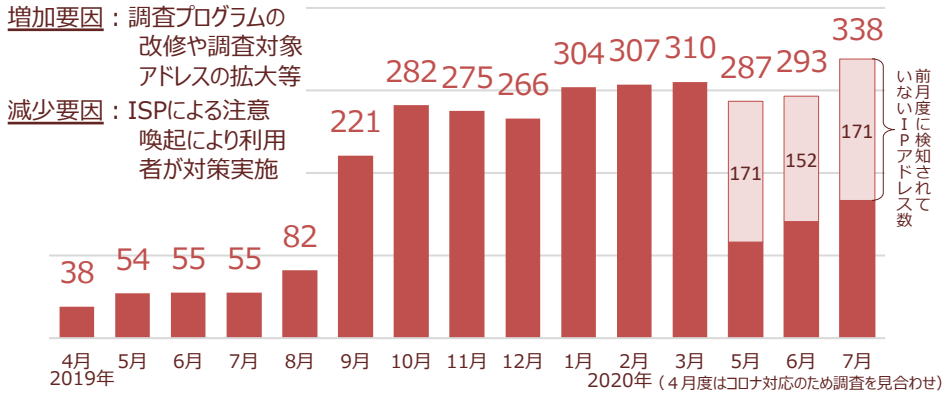
NOTICE注意喚起の取組結果

注意喚起対象としてISPへ通知したもの*

３３８件（６月度:293件）

（参考） 2020年度の累積件数：918件（2019年度：2,249件）
ID・パスワードが入力可能だったもの：11.7万件

*) 特定のID・パスワードによりログインできるかという調査をおおむね月に1回実施し、ログインでき、注意喚起対象となったもの（ユニークIPアドレス数）



NICTER注意喚起※の取組結果

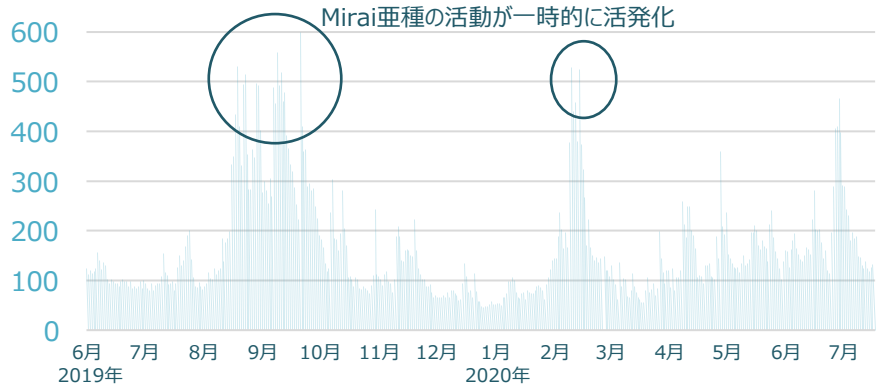
※マルウェアに感染しているIoT機器の利用者への注意喚起

注意喚起対象としてISPへ通知したもの**

１日平均２０９件（６月度:167件）

（参考） 期間全体での値： １日平均163件
最小：46件(2020/1/9)／最大：598件(2019/10/5)

**) NICTERプロジェクトによりマルウェアに感染していることが検知され、注意喚起対象となったもの（ユニークIPアドレス数）

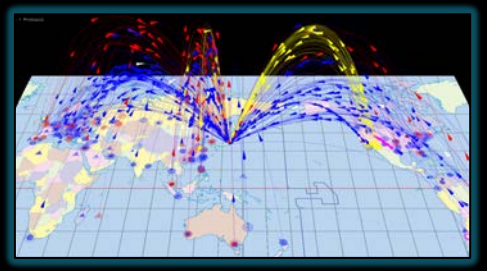


https://notice.go.jp/docs/status202007.pdf

Web媒介型攻撃対策

Web-based **A**ttack **R**esponse with **P**ractical and **D**eployable **R**esearch Initiati**VE**

無差別型攻撃対策



インシデント分析センタ
NICTER

対サイバー攻撃アラートシステム
DAEDALUS

Web媒介型攻撃対策

WARPDRIVE

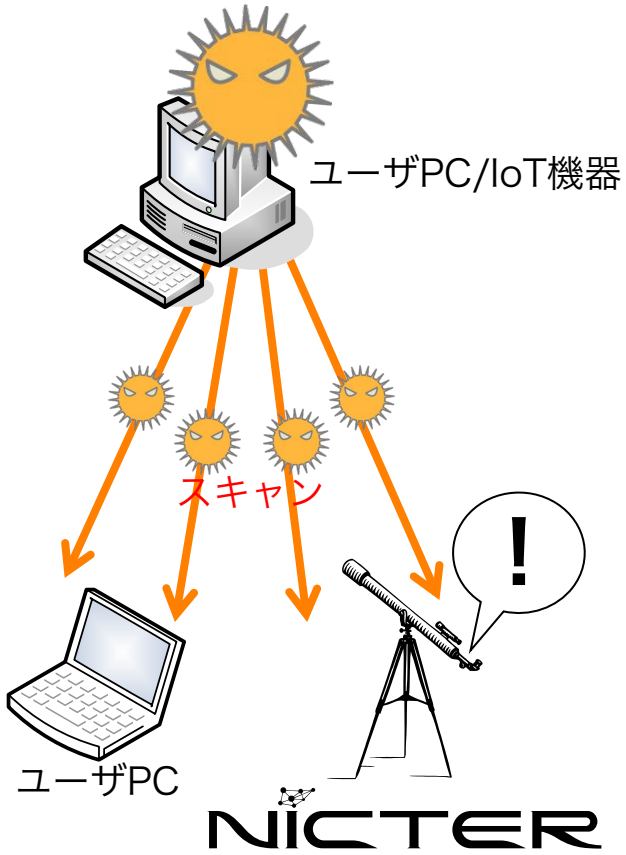
サイバー攻撃統合分析プラットフォーム
NIRVANA改

脆弱性管理プラットフォーム
NIRVANA改弐

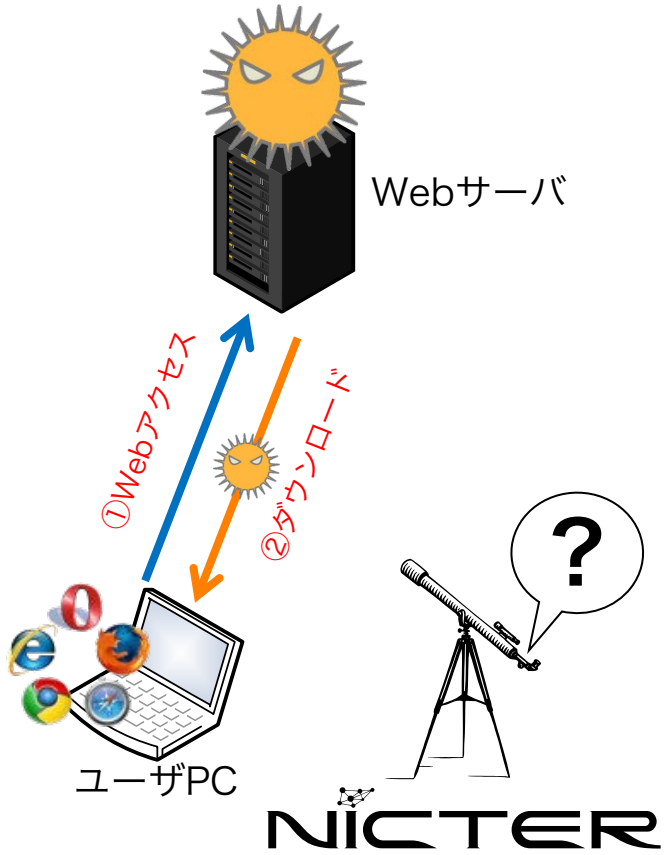
標的型攻撃対策

ワーム型マルウェアとWeb媒介型攻撃の違い

ワーム型マルウェア
（リモートエクスプロイト型マルウェア）



Web媒介型攻撃
（ドライブ・バイ・ダウンロード攻撃）



WARPDRIVE

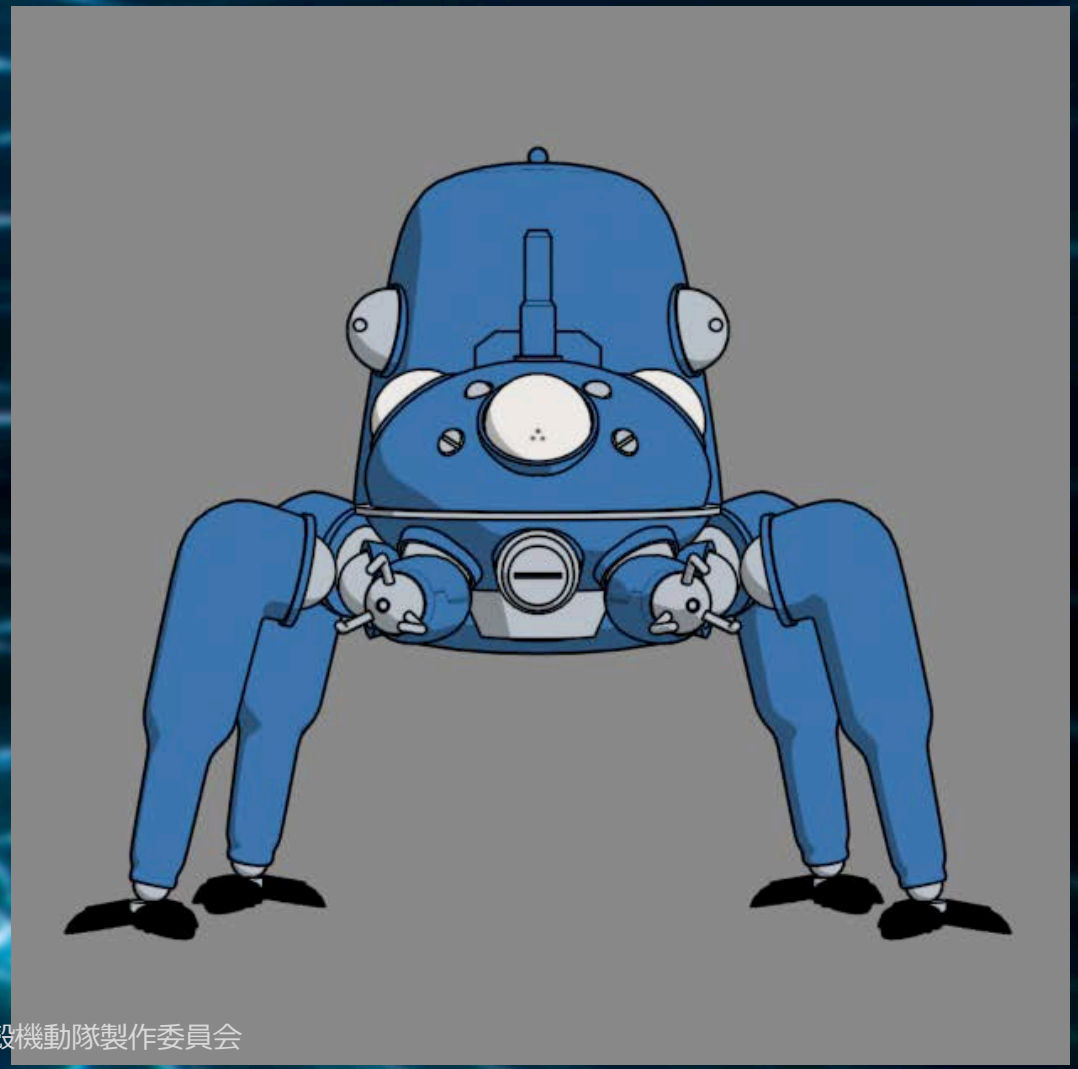
Web-based Attack Response with Practical and Deployable Research InitiatiVE

NICT委託研究『Web媒介型攻撃対策技術の実用化に向けた研究開発』

KDDI総合研究所、セキュアブレイン、横浜国立大学、神戸大学、構造計画研究所、金沢大学、岡山大学

タチコマ

士郎正宗によるSF漫画**「攻殻機動隊」**を原作とし制作されたアニメ「攻殻機動隊S.A.C.」シリーズに登場する自律走行可能な思考戦車。高度な人工知能を搭載しており、操縦者なしでも任務を遂行することができ、電脳空間においては情報収集や電脳戦のサポートを行う。



タチコマ as a ...

1. センサ
2. アクチュエータ
3. コミュニケータ

WARPDRIVE

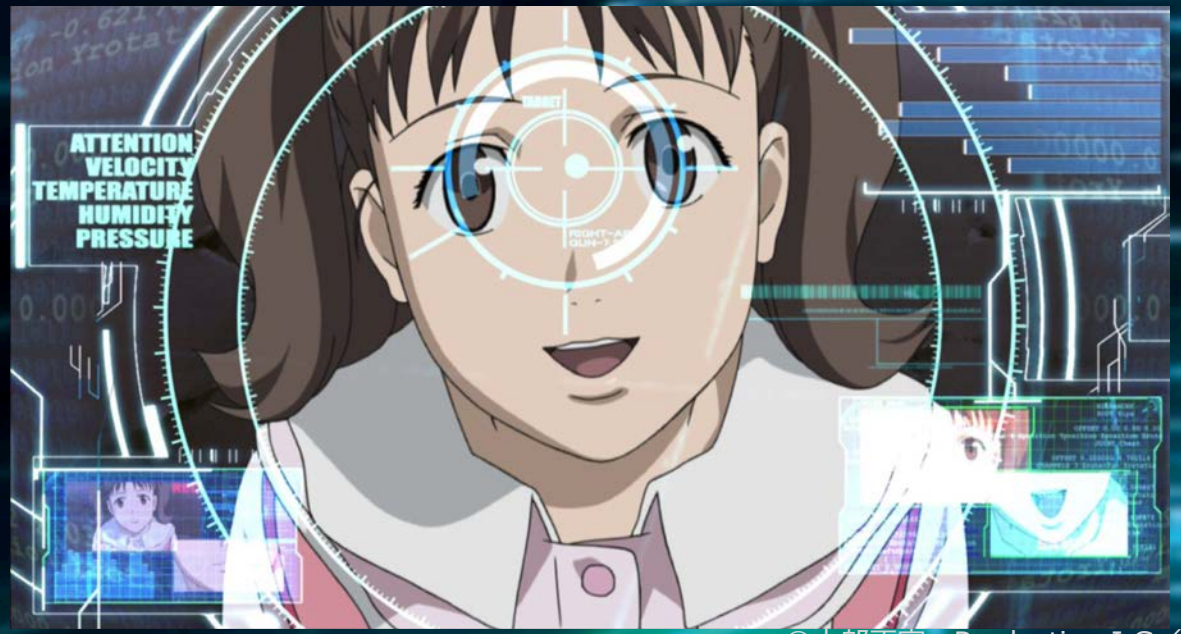
Web-based Attack Response with Practical and Deployable Research InitiatiVE

NICT委託研究『Web媒介型攻撃対策技術の実用化に向けた研究開発』

KDDI総合研究所、セキュアブレイン、横浜国立大学、神戸大学、構造計画研究所、金沢大学、岡山大学

(1) ユーザのコンピュータに「タチコマ」をインストール

攻殻機動隊S.A.C.に登場するAI「タチコマ」を電脳空間にリアライズ。
Web媒介型攻撃対策用『タチコマ・セキュリティ・エージェント』を2018年6月1日より無償配布中！



WarpDrive

Web-based Attack Response with Practical and Deployable Research InitiatiVE

NICT委託研究『Web媒介型攻撃対策技術の実用化に向けた研究開発』

KDDI総合研究所、セキュアブレイン、横浜国立大学、神戸大学、構造計画研究所、金沢大学、岡山大学

(2)「タチコマ」たちが並列化し Web空間を大規模観測

1万人規模のPCにインストールされた「タチコマ」たちがユーザのWebアクセスを大規模観測。

並列化（情報集約、横断分析、新機能展開等）により「タチコマ」が成長！

WARPDRIVE

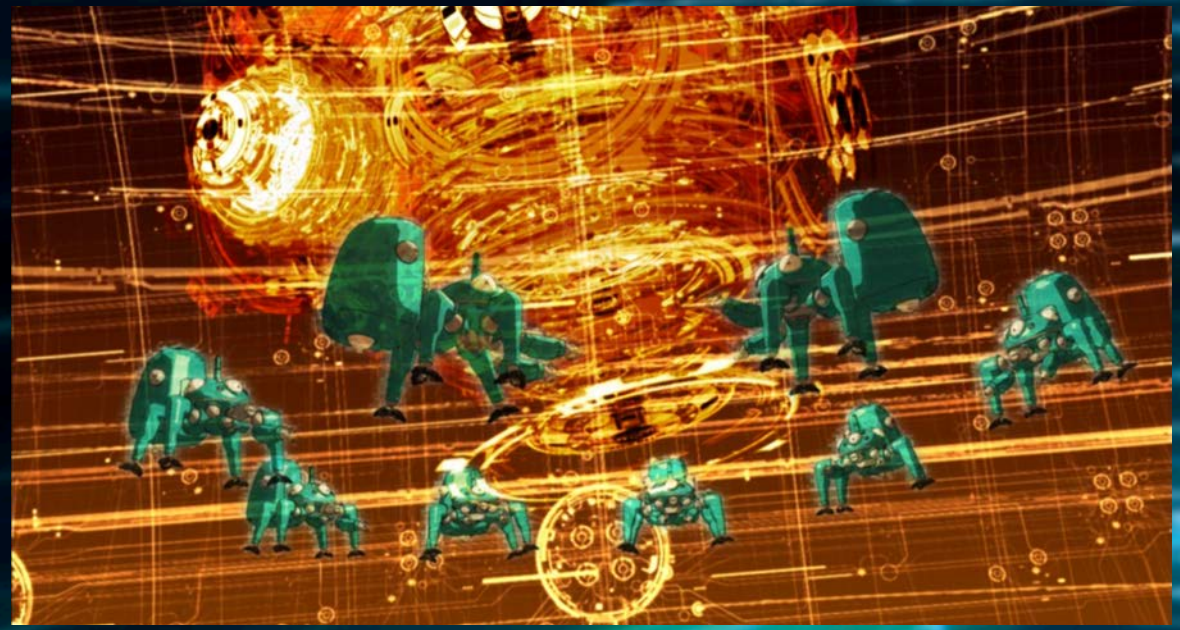
Web-based Attack Response with Practical and Deployable Research InitiatiVE

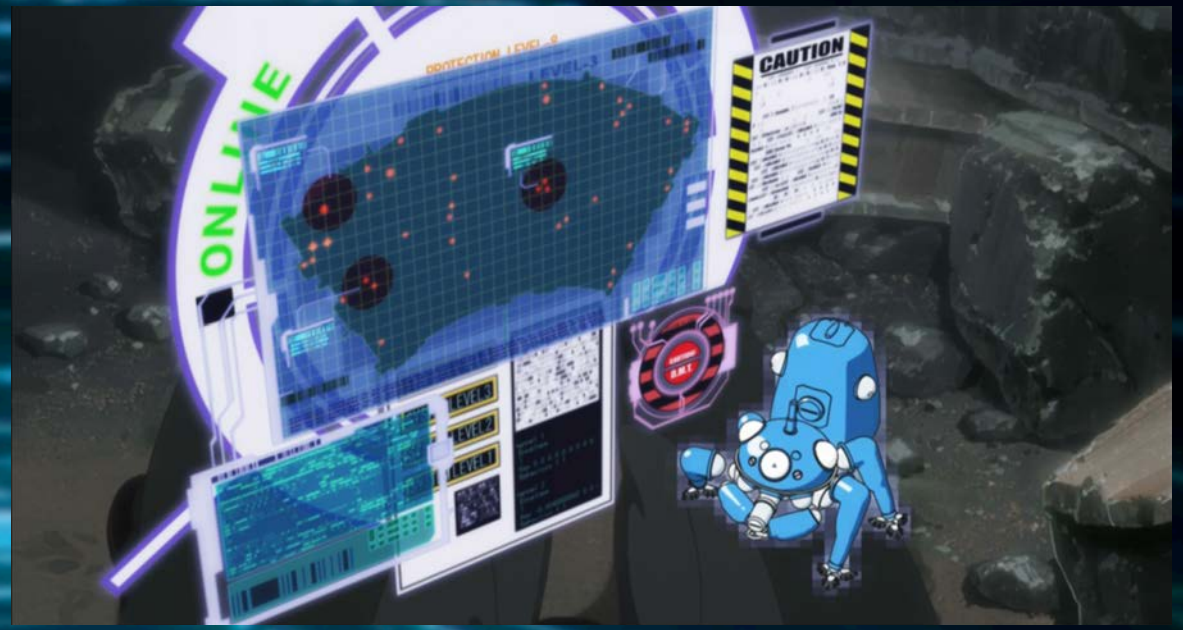
NICT委託研究『Web媒介型攻撃対策技術の実用化に向けた研究開発』

KDDI総合研究所、セキュアブレイン、横浜国立大学、神戸大学、構造計画研究所、金沢大学、岡山大学

(3) 悪性サイト検知時には「タチコマ」が防壁展開 アクセスをブロックしユーザに警告

Web媒介型攻撃検知時には「タチコマ」が防壁展開し、悪性Webサイトへのアクセスをブロック。
「タチコマ」をインターフェイスにしてユーザに警告やアドバイスが届きます！





WarpDrive

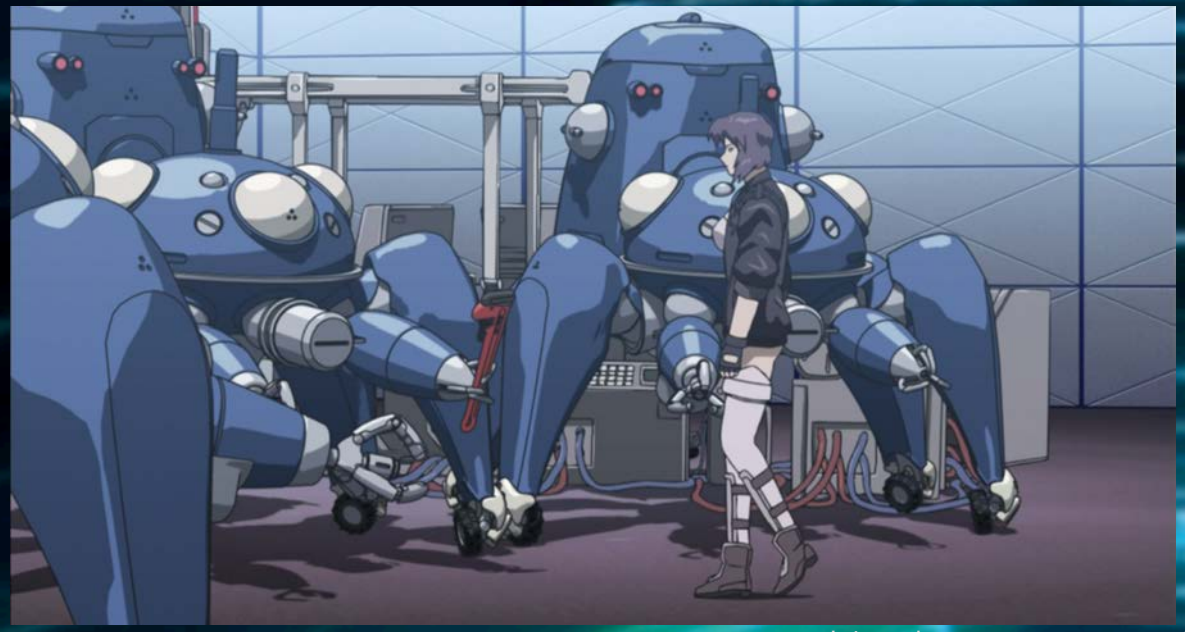
Web-based Attack Response with Practical and Deployable Research InitiatiVE

NICT委託研究『Web媒介型攻撃対策技術の実用化に向けた研究開発』

KDDI総合研究所、セキュアブレイン、横浜国立大学、神戸大学、構造計画研究所、金沢大学、岡山大学

(4) スマートフォンやIoT機器にも順次展開

WarpDriveプロジェクトではスマートフォンやIoT機器（ホームルータ、Webカメラ等）にも
セキュリティ対策を順次展開。2020年3月16日Android向け『タチコマ・モバイル』の無償配布開始！



WarpDrive

Web-based Attack Response with Practical and Deployable Research InitiatiVE

NICT委託研究『Web媒介型攻撃対策技術の実用化に向けた研究開発』

KDDI総合研究所、セキュアブレイン、横浜国立大学、神戸大学、構造計画研究所、金沢大学、岡山大学

タチコマ・モバイル

- Android版タチコマセンサによってスマートフォン経由のWebアクセスを大規模観測
- タチコマとの対話でセキュリティ意識の向上を図る『タチコマの問い』
- 不正サイトやスパムメールの報告機能

WARPDRIVE

Web-based Attack Response with Practical and Deployable Research InitiatiVE

NICT委託研究『Web媒介型攻撃対策技術の実用化に向けた研究開発』

KDDI総合研究所、セキュアブレイン、横浜国立大学、神戸大学、構造計画研究所、金沢大学、岡山大学

電脳空間における

タチコマ・リアライズ

https://warpdrive-project.jp/